Index to Volume 12

BELLARE, M.: Translucent Cryptography—An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transfer 117
BERNSTEIN, D. J.: How to Stretch Random Functions: The Security of Protected Counter Sums 185
BIHAM, E.: Cryptanalysis of Triple Modes of Operation 161
BLUNDO, C.: On a Fallacious Bound for Authentication Codes 155
BLUNDO, C.: On the Contrast in Visual Cryptography Schemes 261
BURMESTER, M.: Divertible and Subliminal-Free Zero-Knowledge Proofs for Languages 197
DE SANTIS, A.: *see* BLUNDO, C. 155, 261
DESMEDT, Y. G.: *see* BURMESTER, M. 197
HALEVI, S.: Efficient Commitment Schemes with Bounded Sender and Unbounded Receiver 77
ITOH, T.: *see* BURMESTER, M. 197
JOYE, M.: Chinese Remaindering Based Cryptosystems in the Presence of Faults 241
KUROSAWA, K.: *see* BLUNDO, C. 155
LENSTRA, A. K.: *see* JOYE, M. 241
NAOR, M. : On the Construction of Pseudorandom Permutations: Luby–Rackoff Revisited 29
OGATA, W.: *see* BLUNDO, C. 155
QUINN, K. A. S.: Bounds for Key Distribution Patterns 227
QUISQUATER, J.-J.: *see* JOYE, M. 241
REINGOLD, O.: *see* NAOR, M. 29
RIVEST, R. L.: *see* BELLARE, M. 117
ROGAWAY, P.: Bucket Hashing and Its Application to Fast Message Authentication 91
SAKURAI, K.: *see* BURMESTER, M. 197
SHIZUYA, H.: *see* BURMESTER, M. 197
SHOUP, V.: On the Security of a Practical Identification Scheme 247
SIKSEK, S.: *see* SMART, N. P. 67
SMART, N. P.: A Fast Diffie–Hellman Protocol in Genus 2 67
SMART, N. P.: Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic 141
SMART, N. P.: The Discrete Logarithm Problem on Elliptic Curves of Trace One 193
STINSON, D. R.: *see* BLUNDO, C. 261
VAN OORSCHOT, P. C.: Parallel Collision Search with Cryptanalytic Applications 1
WIENER, M. J.: *see* VAN OORSCHOT, P. C. 1